



# Department of Homeland Security Daily Open Source Infrastructure Report for 15 August 2006

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](#)

<http://www.dhs.gov/>

## Daily Highlights

- WCAV TV reports Louisa County, Virginia, sheriffs say thieves have been stealing copper at alarming rates from CSX utility poles along the railroad tracks; the railroad is losing thousands of dollars in personal property with these thefts. (See item [16](#))
- The Department of Homeland Security has lowered the aviation threat level from RED to ORANGE for flights from the United Kingdom to the United States; the threat level remains at ORANGE, or "High," for all U.S. domestic and international flights. (See item [17](#))
- The U.S. Conference of Mayors has released a report discussing the state of disaster preparedness in America's cities, with survey responses received from 183 cities representing 38 states, the District of Columbia, and Puerto Rico. (See item [33](#))

## DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *August 14, Associated Press* — **California wildfire damages power substation.** Fire crews fought back a blaze spreading through hillside brush early Monday, August 14, after it temporarily closed a major freeway and knocked out electricity to more than 4,000 homes along the northern edge of Los Angeles County. The blaze had scorched more than 5 1/2 square

miles, and was less than a quarter contained, said Los Angeles County Fire Inspector Sam Padilla. The blaze broke out Sunday and damaged a Southern California Edison substation and at least six power lines, company spokesperson Jeremy Rawitch said. At one point, an estimated 4,450 homes around Gorman were without power. By Sunday night, power was restored to all but 75 customers, Rawitch said.

Source: <http://www.oregonlive.com/newsflash/national/index.ssf?/base/national-69/115556454240460.xml&storylist=ornational>

2. *August 14, Mainichi Daily News (Japan)* — **Tokyo blackouts widespread due to crane damaging power cables.** The scale of the Monday, August 14, power cuts in the Tokyo metropolitan area to approximately 1.39 million people was widespread because two sets of power cables were damaged by a crane floating on a barge on the Kyu Edogawa River. Tokyo Electric Power Co. officials said that each of the two groups of power cables is designed to continue power supply if one of them is damaged. But electricity was completely cut on Monday morning because both sets of cables, each consisting of three lines, were damaged. A similar accident occurred on November 22, 1999, when a Self-Defense Force airplane cut power cables on the bank of the Iruma River in Sayama, Saitama Prefecture. Power supply was cut to about 800,000 households in Tokyo and southern Saitama Prefecture at that time. Technology critic Kiyoshi Sakurai said, "Power companies often have measures against the cutting of power cables near users' homes and against lightening. But Monday's accident was unexpected."

Source: [http://mdn.mainichi-msn.co.jp/national/news/20060814p2a00m0n\\_a015000c.html](http://mdn.mainichi-msn.co.jp/national/news/20060814p2a00m0n_a015000c.html)

3. *August 14, Canadian Press* — **Repeat of major blackout unlikely, experts say.** Three years to the day after 50 million people in Ontario and parts of the North Eastern U.S. were plunged into darkness, energy watchdogs say improved reliability measures make a repeat of the blackout unlikely but caution that stepped up conservation efforts are needed. Says Tom Adams of Energy Probe, "All of the major transmission utilities have invested significant dollars in upgrading their system." While a 2004 audit by the North American Electric Reliability Council found Ontario's Independent Electricity System Operator to be a model for other system operators, the blackout was a catalyst for improvement to the province's system, Adams said. Hydro One has put about \$277 million for grid maintenance in its 2007 budget, which is \$100 million more than in 2003. Planned projects were kick-started by the blackout such as the construction of a \$45 million underground transmission line in Toronto that Adams said will improve reliability in the power grid across the Greater Toronto Area. New laws in the U.S. are also improving reliability, Adams said. Rules, such as the distance a tree must be from a transmission line, will now be mandatory across the country. The council is seeking similar approval from Canadian jurisdictions.

Source: [http://toronto.ctv.ca/servlet/an/local/CTVNews/20060814/ontario\\_blackout\\_060814/20060814?hub=TorontoHome](http://toronto.ctv.ca/servlet/an/local/CTVNews/20060814/ontario_blackout_060814/20060814?hub=TorontoHome)

[[Return to top](#)]

## **Chemical Industry and Hazardous Materials Sector**

4. *August 13, Associated Press* — **Homes evacuated after fire at paint factory.** A fire at a paint-manufacturing plant on Sunday, August 13, in Caldwell County, TX, forced the

evacuation of about 20 homes. No injuries were reported.

Source: [http://www.zwire.com/site/news.cfm?newsid=17050152&BRD=1994&PAG=461&dept\\_id=339096&rft=6](http://www.zwire.com/site/news.cfm?newsid=17050152&BRD=1994&PAG=461&dept_id=339096&rft=6)

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

5. *August 14, Aviation Now* — **Air Force looks to beef up capability against insurgents and terrorists.** The Air Force has launched an initiative to look at developing or modifying its fleet structure to better fight insurgencies and terrorist operations. While the service itself has remained officially mum on the subject, Air Force leadership has been reaching out to experts in the field to see what needs to be done to better equip the service for such battles and operations. The service recently directed the RAND Corp. to do a study on counter insurgency (COIN) aircraft needs as part of RAND's Project Air Force program. RAND completed the unclassified report — "COIN Aircraft Systems for the USAF and Friendly States Facing Insurgencies" — in June. In the study, RAND says there will be a need for such a capability for some time to come. The Air Force is flying COIN missions with aircraft designed for other purposes, but aircraft specifically designed for COIN would be better, according to RAND. Some of their advantages, the report says, include effectiveness, operating economics, flexibility to perform other missions, and the ability to equip friends and allies confronting insurgencies. Such a study and capability are needed, especially now, analysts say.

Source: [http://www.aviationnow.com/avnow/news/channel\\_aerospacedaily\\_story.jsp?id=news/USAF08146.xml](http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/USAF08146.xml)

[\[Return to top\]](#)

## **Banking and Finance Sector**

6. *August 14, Finextra* — **UK bank account details for sale in Nigeria.** The BBC says an investigation into the risk of identity theft from old PCs by its Real Story program has found that scammers in Nigeria are able to access Internet banking data stored on recycled computers sent from United Kingdom (UK) council recycling points to Africa. Scammers can access confidential data on a PC's hard disk very easily if the drive is not fully wiped.
- Source: <http://finextra.com/fullstory.asp?id=15720>
7. *August 14, Associated Press* — **Mideast cease-fire boosts Wall Street.** Wall Street welcomed a cease-fire between Israel and Lebanon Monday, August 14, sending stocks higher as oil prices also dropped sharply. With no economic data and little corporate news of note, investors saw the cease-fire as a buying opportunity after last week's losses. Crude futures fell as traders saw less risk of a supply disruption in the Middle East after the United Nations-mandated cease-fire took effect. A barrel of light crude was quoted at \$73.05, down \$1.30, on the New York Mercantile Exchange. However, Wall Street's rally could be short lived with two major inflation reports due later in the week: the Labor Department's producer price index on Tuesday, August 15, and the consumer price index on Wednesday, August 16. With the Federal Reserve warning the markets last week that inflation remains a concern, stocks could revert to

the volatility of recent weeks if incoming economic data shows rising prices on the wholesale or consumer levels.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/08/14/AR2006081400214.html>

8. *August 12, Toledo Blade (OH)* — **Fifth Third Bank warns customers of e-mail con.** Fifth Third Bank in Northwestern Ohio and its online customers are the latest victims of increasingly sophisticated "phishing" schemes that attempt to extract personal information from people who are unaware banks don't ask for it through e-mails. Since early July, would-be thieves have sent fraudulent e-mails claiming Fifth Third's technical department is doing a scheduled software upgrade and asking recipients to click onto a link, where they then are asked to provide personal information. "We have been immune to this for a long time, but now we're a target," said Karen Fraker, senior vice president at the bank. Customers should not reply to the bogus e-mails but contact the bank so they can be tracked, she said.

Source: <http://toledoblade.com/apps/pbcs.dll/article?AID=/20060812/BUSINESS07/608120380/-1/BUSINESS>

9. *August 11, Reuters* — **Bomb plot "wake-up call" in terror finance fight.** The world's top money laundering watchdog on Friday, August 11, called on countries to intensify measures to combat the financing of terrorism in the wake of the United Kingdom bomb plot and called Britain's efforts exemplary. Alain Damais, executive secretary of the Paris-based Financial Action Task Force (FATF), said the thwarted attack served as a reminder to countries to intensify anti-terror finance measures designed to choke off funds to militants. "This is again a kind of wake-up call for all the countries around the world to implement the measures," Damais said in a telephone interview. "The financial system can always be abused." Earlier on Friday, Britain named 19 people suspected of an Islamist plot to blow up transatlantic airliners and ordered their assets frozen, a day after police said they had foiled "murder on an unimaginable scale". Damais cheered the Bank of England for ordering the freeze, saying it demonstrated that countries now know how to respond to terrorism threats using tools agreed to in recent years by the FATF and adopted by member countries.

Source: [http://today.reuters.com/news/articlenews.aspx?type=reutersE&storyID=2006-08-11T153609Z\\_01\\_L11487210\\_RTRUKOC\\_0\\_US-SECURITY-FATE.xml](http://today.reuters.com/news/articlenews.aspx?type=reutersE&storyID=2006-08-11T153609Z_01_L11487210_RTRUKOC_0_US-SECURITY-FATE.xml)

10. *August 11, Continuity Central (United Kingdom)* — **Reserve Bank of India provides business continuity instructions to banks.** The Reserve Bank of India has issued guidelines to all scheduled banks in the country, informing them of the business continuity measures that must be in place to ensure quick restoration of banking services in areas affected by natural calamities. The Reserve Bank says that banks have a duty to provide customers with uninterrupted access to bank accounts and must facilitate the opening of new accounts by persons affected by natural disasters; especially so that people can quickly receive relief and aid given by the Indian government and other agencies. The business continuity guidelines also cover measures to be taken by banks to ensure continuity of other services; such as check clearing services and the supply of cash.

Reserve Bank of India's guidelines:

<http://www.rbi.org.in/scripts/NotificationUser.aspx?Id=3056& Mode=0>

Source: <http://continuitycentral.com/news02721.htm>

## **Transportation and Border Security Sector**

11. *August 14, CNN* — **Mobile phone scare on BA flight.** A British Airways (BA) flight from London to New York turned back on Sunday, August 13, when a mobile phone was found on board. Flight BA179 returned to the airport after the mobile phone was heard ringing at the back of the plane. None of the 217 passengers on board the plane appeared to own the phone. Mobile phones, along with all items of hand luggage except the bare essentials, were banned from flights Thursday, August 10, after a plot to bomb transatlantic flights was foiled. BA's security team at Heathrow were consulted about the mobile phone incident and decided it was safe for the plane to continue its journey. However, the captain turned back as a precautionary measure.  
Source: <http://edition.cnn.com/2006/TRAVEL/08/14/flight.returned/>
12. *August 14, Associated Press* — **Flight evacuated at Los Angeles International Airport after reports of suspicious item.** Police safely evacuated an Alaska Airlines flight on Monday, August 14, after a report that a "suspicious item" was found on board, a Los Angeles International Airport spokesperson said. Airport police received notification at 8:20 a.m. PDT that there was a suspicious item on board a plane which originated in Guadalajara, Mexico, said airport spokesperson Nancy Castles. She said she did not know what the item was and did not release any additional details. The plane landed without incident just before 9 a.m., Castles said, and all 125 passengers were transported to the terminal in buses after the plane stopped in a remote area of the airport. A Los Angeles Police bomb squad and the FBI will search the plane, she said.  
Source: <http://www.cnn.com/2006/TRAVEL/08/14/mexico.flight.ap/index.html>
13. *August 14, Associated Press* — **Coast Guard increases security around Mackinac Bridge.** The U.S. Coast Guard has increased patrols near the bridge connecting Michigan's upper and lower peninsulas after prosecutors said they believe three men jailed on terrorism charges were targeting the five-mile-long span. Tuscola County Prosecutor Mark E. Reese said investigators believe the men were targeting the Mackinac Bridge. The men were arrested Friday outside a Wal-Mart stores in Caro, about 80 miles north of Detroit, after purchasing 80 cell phones. Authorities say the men had about 1,000 cell phones in their van.  
Source: <http://www.cnn.com/2006/US/08/14/mackinac.ap/index.html>
14. *August 14, Associated Press* — **Oregon train derailment traced to heat wave.** Union Pacific officials blamed the weather for last month's derailment of 37 freight cars in southern Oregon. Union Pacific spokesperson James Barnes said the extreme heat buckled the railroad track the runs next to Upper Klamath Lake. The derailment halted rail operations in some parts of the West Coast for three days. Though rail service has resumed, most of the cars remain next to the track. When damaged cars cannot be placed back on the rails, they must be individually broken down and hauled away, Barnes said. The Klamath Basin had an unusually prolonged heat spell in the weeks before the derailment. Crews had started rail upgrade work in the general area before the accident. The crews were south of the site, however, so it's unclear if their work could have prevented the derailment.



Source: <http://www.oregonnews.com/article/20060814/NEWS/60814005>

15. *August 14, Associated Press* — **Cruise ship employee accused of stealing \$400,000 in cash.**

A former Princess Cruises employee accused of stealing \$400,000 from a ship's safe was charged on Friday, August 11, in a Ketchikan, AK, court. Elisha Cuffe, 32, who had worked for the company for 10 years, had taken the money to her cabin and stashed it in a shoebox at the foot of her bed. The Australia resident, whose job as a purser exposed her at times to \$1.5 million in cash, was charged with first-degree theft. Cuffe told authorities she noticed the ship's computer was not showing the correct amount of money in the safe, so she took it. She told them she had not been planning to take the money off the ship. The ship's staff found the money during an internal investigation on Thursday, August 10. The ship's officers told authorities that in May they had started noticing some accounting discrepancies on board.

Source: [http://www.usatoday.com/travel/news/2006-08-14-cruise-theft\\_x.htm](http://www.usatoday.com/travel/news/2006-08-14-cruise-theft_x.htm)

16. *August 14, WCAV TV (VA)* — **Virginia CSX hit by copper thieves.** With copper worth nearly \$4 per pound criminals can make a pretty penny selling it and they are going to great lengths to get it. "Copper is bringing in a lot of money right now. It's over \$3 a pound," said Patrick Sheridan of the Louisa County (VA) Sheriff's Department. That's why Louisa County sheriff's department says thieves have been stealing it at alarming rates from these CSX utility poles along the railroad tracks. CSX reports stolen copper wire in Louisa, Cismont, and in Scottsville. The railroad is losing thousands in personal property so when operators saw someone suspicious on the tracks Wednesday, August 9, they called the sheriff. "We hid in the woods and while hiding in the woods we were able to watch him pull down the copper wire from the poles, cut it down, roll it into small rolls and set it on the tracks," said Sheridan.

Source: <http://www.charlottesvilleneewsplex.tv/news/headlines/3553512.html>

17. *August 13, Department of Homeland Security* — **Department of Homeland Security adjusts threat level from Red to Orange for on-bound flights from the UK.** Effective immediately, the Department of Homeland Security has announced an adjustment in the aviation threat level from RED to ORANGE for flights from the United Kingdom to the United States. There will not be any operational changes for domestic flights in the United States. Thus, the U.S. threat level remains at ORANGE, or "High," for all domestic and international flights. The ban on liquids and gels in carry on baggage remains in full effect. While the threat level drops from RED to ORANGE on United Kingdom flights bound to the United States, passengers can expect enhanced measures to remain in place for these flights, including additional restrictions on hand luggage and gate check inspections. Domestically, U.S. travelers should expect to see an increase in visibility and use of canine detection teams. Random inspections of bags at departure gates will continue. Also, the Transportation Security Administration has announced slight modifications to its current security procedures, which can be viewed at

<http://www.tsa.gov>

Source: [http://www.dhs.gov/dhspublic/interapp/press\\_release/press\\_re lease\\_0981.xml](http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0981.xml)

18. *August 12, Associated Press* — **Smoking suitcase forces DFW terminal evacuation.** Portions of a terminal at Dallas-Fort Worth (DFW) International Airport were evacuated for about three hours on Saturday, August 12, while fire and police officials inspected a suitcase emitting smoke and liquid. Police and fire officials examined the bag and used an X-ray. They found no hazardous materials, said DFW fire chief Alan Black. Authorities eventually tracked down the

bag's owner and determined the suspicious item was an aerosol hairspray can.

Source: <http://www.chron.com/disp/story.mpl/metropolitan/4113069.html>

[\[Return to top\]](#)

## **Postal and Shipping Sector**

19. *August 14, Government Computer News* — **Postal branch seeks research on advanced search tools.** The U.S. Postal Service is conducting market research for a commercially available advanced search and analysis tool for data and text material. In a recent notice, the U.S. Postal Inspection Service (USPIS) said the search tool must be able to parse and analyze criminal information that will direct investigative resources in an efficient manner. Responses are due August 25. The USPIS is the Postal Service's law enforcement branch responsible for enforcing nearly 200 federal laws.

Source: [http://www.gcn.com/online/vol1\\_no1/41625-1.html](http://www.gcn.com/online/vol1_no1/41625-1.html)

20. *August 11, American City Business Journals* — **Rickenbacker ranked among fastest growing cargo airports.** In the world of moving air cargo, Columbus, Ohio's Rickenbacker International Airport is in the same category as Malaysia's Subang Airport and Nigeria's Lagos Airport. Air Cargo World magazine rated Rickenbacker as the 17th fastest growing airport for shipping freight in its July issue. The Columbus Regional Airport Authority attributes the increase to business AirNet Systems Inc. brought when it relocated its express shipping operations from Port Columbus International Airport to Rickenbacker in February.

Source: <http://biz.yahoo.com/bizj/060811/1330586.html?.v=1>

[\[Return to top\]](#)

## **Agriculture Sector**

21. *August 14, Illinois Ag Connection* — **Illinois launches fight against ash borer.** Illinois will wage a multi-million dollar fight against an ash tree beetle — the emerald ash borer — to prevent the devastation state officials recently saw in Michigan. "There were giant (ash) tree skeletons. The big branches were there, but the foliage and small branches were gone," said Warren Goetsch of the Illinois Department of Agriculture (IDOA). Governor Rod Blagojevich has created a scientific advisory team to help IDOA, the lead agency implementing Illinois' emergency plan. Illinois has about 130 million ash trees.

Emerald ash borer information: <http://www.emeraldashborer.info/>

Source: <http://www.illinoisagconnection.com/story-state.cfm?Id=698&y r=2006>

22. *August 14, Agricultural Research Service* — **New form of fusarium wilt could pose threat to watermelon crop.** In separate studies, scientists with the Agricultural Research Service (ARS) in Lane, OK, and at the University of Maryland (UM) have identified a new, more aggressive race of the fungus that causes Fusarium wilt in watermelon. This disease is one that all melon farmers dread seeing. It can attack plants at any stage of growth, leaving young seedlings lifeless, or mature plants fruitless with nothing to show but shriveled and yellowing leaves. The scientists discovered a new race of the fungus *Fusarium oxysporum* that causes Fusarium wilt.

Their findings were presented last week at the joint meeting of the American Phytopathology Society and Mycological Society of America, in Quebec City, Canada. The new race was found while monitoring watermelon plants in fields in Oklahoma. Three distinct races of *Fusarium* are known to cause wilt in melons. Plant breeders have developed watermelon varieties that can fend off Races 0 and 1 fairly well. And, luckily, Race 2 — for which there are no resistant commercial cultivars — isn't competitive in the soil environment.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

- 23. *August 11, Ohio Ag Connection* — Emerald ash borer discovered in Ohio.** Ohio Department of Agriculture Director Fred Dailey Thursday, August 10, announced a new discovery of Emerald ash borer (EAB), an ash tree-killing insect from Asia, in Miami and Wyandot counties. This marks the first EAB discovery in both counties, which officials have quarantined to halt the movement of ash tree material and hardwood firewood, which could harbor the pest. EAB surveyors made both discoveries while doing routine detection work in the area. The origin of the infestations is unknown but likely resulted from the movement of firewood, ash tree nursery stock, ash logs, or other ash tree materials. Department surveyors will further investigate the size and origin of the infestations before determining how to proceed. In the meantime, the department has quarantined Miami and Wyandot counties, making it illegal for citizens to move ash trees, parts of ash trees, and all hardwood firewood out of the area. Emerald ash borer information: <http://www.emeraldashborer.info/>  
Source: <http://www.ohioagconnection.com/story-state.cfm?Id=515&yr=2006>

[\[Return to top\]](#)

## **Food Sector**

- 24. *August 10, U.S. Food and Drug Administration* — Alfalfa recalled.** Fullei Fresh of Miami, FL, is recalling its five-ounce containers of alfalfa sprouts because they have the potential to be contaminated with *Salmonella*, an organism which can cause serious and sometimes fatal infections in young children, frail, or elderly people, and others with weakened immune systems. Healthy persons infected with *Salmonella* often experience fever, diarrhea, nausea, vomiting, and abdominal pain. In rare circumstances, infection with *Salmonella* can result in the organism getting into the bloodstream and producing more severe illnesses such as arterial infections, endocarditis and arthritis. The recalled alfalfa sprouts were distributed statewide in food service establishments. This product was grown and packaged by Fullei Fresh, and distributed by produce companies. No illnesses have been reported to date in connection with this problem. The potential for this contamination was noted after random testing by the company revealed the presence of *Salmonella* in one cup of finished product.  
Source: [http://www.fda.gov/oc/po/firmrecalls/fullei08\\_06.html](http://www.fda.gov/oc/po/firmrecalls/fullei08_06.html)

[\[Return to top\]](#)

## **Water Sector**

Nothing to report.

[\[Return to top\]](#)



## **Public Health Sector**

25. *August 14, Agence France–Presse* — **China confirms 14th bird flu fatality.** China's health ministry has confirmed a new fatal human case of bird flu, a 62-year-old man who died from the virus last month to become the nation's 14th confirmed fatality. The victim was from Jimsar County in the northwest region of Xinjiang, the ministry said in a statement Monday, August 14. It said the man fell ill on June 19 and died on July 12, and that initial laboratory tests aimed at checking if he had succumbed to the H5N1 avian flu virus had been inconclusive. People who had been in contact with him have been placed under observation, the ministry said. The man is the 21st human patient to be confirmed by China's health authorities.  
Source: [http://news.yahoo.com/s/afp/20060814/hl\\_afp/healthfluchina\\_060814134023;\\_ylt=AtvqTywRiy0YuvocA6mEd.eJOrgF;\\_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--](http://news.yahoo.com/s/afp/20060814/hl_afp/healthfluchina_060814134023;_ylt=AtvqTywRiy0YuvocA6mEd.eJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--)
26. *August 14, Laboratory Talk* — **Asian biosafety short of international standards.** A report recently released by Sandia National Laboratories shows that researchers in 16 Asian countries often use insufficient biosafety practices. Biosafety Level (BSL) 2 practices are often employed for research involving BSL 3 agents. Nearly two-thirds of respondents investigating Japanese encephalitis, avian influenza, and severe acute respiratory syndrome (SARS) — which are all BSL 3 agents — perform their research under BSL 2 specifications. For this report, 300 scientists were surveyed to assess the current practices employed in studying infectious agents by laboratories located in 16 Asian countries — segmented by the level of biotechnological sophistication.  
Report: <http://www.biosecuritycodes.org/docs/Asia%20summary%20SAND%20report%20final.pdf>  
Source: <http://www.laboratorytalk.com/news/bin/bin142.html>
27. *August 14, Associated Press* — **Indonesian bird flu patient refuses treatment.** Indonesia's latest bird flu patient checked out of hospital after spending just a night there, while his cousin died last week showing symptoms of the virus but was not tested in time, health officials said Monday, August 14. Umar Aup was admitted to a hospital in West Java province Wednesday, August 9, and left the next day on the orders of his family. Villagers said Aup and his cousin collected the carcasses of around 100 chickens that died suddenly last week and fed them to dogs. Laboratory tests have confirmed Aup has the virus. The case shows the challenges facing health workers dealing with bird flu in Indonesia, a sprawling country which last week became the country worst hit by the virus. The virus is rampant among Indonesia's billions of backyard chickens. Slaughtering often isn't carried out following outbreaks, vaccination is spotty and surveillance is weak, international experts say.  
Source: [http://www.thejakartapost.com/detailgen.asp?fileid=20060814\\_154128&iREC=0](http://www.thejakartapost.com/detailgen.asp?fileid=20060814_154128&iREC=0)
28. *August 12, Agence France–Presse* — **India declares itself bird–flu free.** India announced it was free of bird flu, six months after the country first reported an outbreak of the deadly virus. "India has declared that it has regained its status as an avian influenza–free country," the Indian health ministry said in a statement. "There has been no further outbreak of avian influenza in India after April 18." The disease was first confirmed in chickens in western India in February, leading to the culling of more than a million birds by health authorities.

Source: [http://news.yahoo.com/s/afp/20060812/hl\\_afp/healthfluindia\\_060812170557;\\_ylt=ApioFCBYUyYW\\_KR5u5Y\\_zUiJOrgF;\\_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--](http://news.yahoo.com/s/afp/20060812/hl_afp/healthfluindia_060812170557;_ylt=ApioFCBYUyYW_KR5u5Y_zUiJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--)

[[Return to top](#)]

## **Government Sector**

29. *August 13, CNN* — **Machete-wielding woman outside White House.** A 32-year-old woman wielding a machete was arrested Sunday, August 13, outside the White House, the Secret Service said. Spokesperson Kim Bruce said Ashwak Saleh was taken into custody and charged with possession of a prohibited weapon after she displayed a 13-inch machete on the sidewalk outside the White House. Witnesses said Saleh was sitting on the sidewalk when she pulled the machete out of a leather sleeve and began sharpening it on the edge of the sidewalk. The witnesses said passersby then alerted Secret Service officers, one of whom approached the woman and told her to "Drop the blade." To that, Saleh said, "What are you going to do — shoot me?"

Source: <http://www.cnn.com/2006/US/08/13/wh.machete/index.html>

[[Return to top](#)]

## **Emergency Services Sector**

30. *August 14, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Update: Atlantic/Gulf of Mexico/Caribbean Sea: A tropical wave accompanied by a weak area of low pressure is located in the vicinity of the Windward Islands. This system has changed little over several days. In addition, a broad non-tropical low pressure area is located several hundred miles east of the northeastern Florida coast. Some slow development is possible over the next couple of days as the system remains nearly stationary. Elsewhere, tropical storm formation is not expected through Tuesday, August 15. Eastern Pacific: The inter-tropical convergence zone that has been under observation for the last few days remains fairly active well south of the Hawaiian islands. However, there are no areas of organized convection within this area that suggest tropical cyclone development. Western Pacific: Tropical Storm 11w (Wukong) and Tropical Depression 12w, tracking toward the coast of Japan, are moving away from U.S. interests.

To view other Situation Updates: <http://www.fema.gov/emergency/reports/index.shtm>

Source: <http://www.fema.gov/emergency/reports/2006/nat081406.shtm>

31. *August 11, PC World* — **Computer grid aims to predict storm surge.** Universities in the southeastern U.S. are building a computer grid designed to help scientists predict storm surges well in advance of an approaching hurricane to give government officials a better idea of when to order evacuations. Improving storm surge forecasting means harnessing large amounts of computing power that can quickly analyze meteorological and oceanographic data needed to develop forecast models. "The real challenge here is to be able to create a product far enough in advance of a storm hitting the coast to actually take action," said Gary Crane, director of IT initiatives for the Southeastern Universities Research Association (SURA). He said surge

forecasts are now accurate about 24 hours ahead of time; one goal is to extend that forecasting window to 72 hours. Crane said the grid has the potential of growing many times in size — depending on the number of other universities that contribute resources to the computing pool behind it.

SURA Website: <http://www.sura.org/home/index.html>

Source: <http://www.pcworld.com/article/id.126713-c.technology/article.e.html#>

32. *August 10, New Scientist* — **Sonification may help warn of volcanic eruption.** Active volcanoes are being made to "sing" by researchers who convert seismic data into frequencies audible to human ears. The technique could make it easier to detect patterns that warn of an eruption. The technique, known as "sonification," is used to help people detect patterns in complex data. Research has shown that people find it easier to detect patterns audibly rather than visually.  
Source: <http://www.newscientist.com/article/dn9711-volcanoes-may-reveal-secrets-through-song.html>
33. *July 26, U.S. Conference of Mayors* — **Five years post 9/11 and one year post Hurricane Katrina: The state of America's readiness.** As the nation approaches the five-year anniversary of the terrorist attacks of September 11 and the one-year anniversary of Hurricane Katrina, the U.S. Conference of Mayors, has released a report discussing the state of disaster preparedness in America's cities. Survey responses were received from 183 cities representing 38 states in the nation, and the District of Columbia and Puerto Rico. Some of the key findings of the survey include: a) when asked have cities received sufficient federal resources to achieve full communications interoperability so that first responders can talk to each other and key assets, 80 percent said no; b) when then asked how far away cities are from having full communications interoperability, the average response was four years; c) when asked how much each city's level of disaster preparedness has improved since 9/11 — with 1 being the lowest and 10 being the highest amount of improvement, the average response was 6.3; d) when asked if cities have recently created or updated an evacuation plan, the average response was 56 percent yes. This number climbed to 73 percent yes for the largest cities.  
Full report: [http://www.usmayors.org/uscm/news/press\\_releases/documents/disasterpreparednesssurvey\\_2006.pdf](http://www.usmayors.org/uscm/news/press_releases/documents/disasterpreparednesssurvey_2006.pdf)  
Source: [http://usmayors.org/uscm/news/press\\_releases/documents/disasterpreparedness\\_072606.pdf](http://usmayors.org/uscm/news/press_releases/documents/disasterpreparedness_072606.pdf)

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

34. *August 13, eWeek* — **Botnet herders attack MS06-040 worm hole.** The first wave of malicious attacks against the MS06-040 vulnerability is underway, using malware that hijacks unpatched Windows machines for use in IRC-controlled botnets. The attacks, which started late Saturday, August 12, use a variant of a backdoor Trojan that installs itself on a system, modifies security settings, connects to a remote Internet Relay Chat (IRC) server and starts listening for commands from a remote hacker, according to early warnings from anti-virus vendors. The Microsoft Security Response Center described the attack as "extremely targeted" and said it appears to be specifically targeting unpatched Windows 2000 machines. According

to the LURHQ Threat Intelligence Group, the attackers are using a variant of the Mocabot trojan that was used in the Zotob worm attack in August 2005. "Amazingly, this new variant of Mocabot still uses the same IRC server hostnames as a command-and-control mechanism after all these months. This may be partially due to the low-profile it has held, but also may be due to the fact that the hostnames and IP addresses associated with the command-and-control servers are almost all located in China," LURHQ said in an advisory.

LURHQ Advisory: <http://www.lurhq.com/mocabot-ms06040.html>

Source: <http://www.eweek.com/article2/0.1895.2002966.00.asp>

35. *August 11, Secunia* — **Linux Kernel multiple vulnerabilities.** Multiple vulnerabilities have been reported in the Linux Kernel, which can be exploited by malicious, local users to cause a denial-of-service, bypass certain security restrictions, and disclose potentially sensitive information.

Vulnerable product: Linux Kernel 2.4.x.

Solution: Update to version 2.4.33: <http://kernel.org/>

Source: <http://secunia.com/advisories/21476/>

36. *August 11, Secunia* — **IBM HMC Apache buffer overflow vulnerability.** IBM has acknowledged a vulnerability in IBM Hardware Management Console (HMC), which can be exploited by malicious people to cause a denial-of-service. The vulnerability is caused due to some boundary errors in the ApacheBench benchmark support program. This can be exploited to cause a buffer overflow via a malicious server.

Vulnerable product: IBM HMC.

Solution: Apply security fix U808917 for version 3.3.7:

[http://www14.software.ibm.com/webapp/set2/subscriptions/pqvc\\_mjd?mode=18&ID=2871](http://www14.software.ibm.com/webapp/set2/subscriptions/pqvc_mjd?mode=18&ID=2871)

Source: <http://secunia.com/advisories/21425/>

37. *August 11, Secunia* — **IBM HTTP Server two vulnerabilities.** IBM has acknowledged two vulnerabilities in IBM HTTP Server, which can be exploited by malicious people to conduct cross-site scripting attacks and potentially compromise a vulnerable system.

Vulnerable product: IBM HTTP Server 1.x.

Solution: Apply PK27875: <http://www-1.ibm.com/support/docview.wss?uid=swg24013080>

Source: <http://secunia.com/advisories/21478/>

38. *August 11, Security Focus* — **Covert channel tool hides data in IPv6.** An independent security researcher showed off an early version of a tool for creating covert channels that, he claims, can pass undetected through most firewalls and intrusion detection systems. The tool, dubbed VoodooNet or v00d00n3t, uses the ability of most computers to encapsulate next-generation network traffic, known as Internet Protocol version 6 (IPv6), inside of today's network communications standard, or IPv4. Because most security hardware appliances and host-based intrusion detection programs have not been programmed to inspect IPv6 packets in depth, data can bypass most network security, said independent security researcher Robert Murphy, who presented the tool at the DEFCON hacking conference last weekend. The tool uses Internet Control Message Protocol version 6, or ICMPv6, to send ping packets from one computer to another, hiding information in certain fields of the packets without violating any existing Internet Request for Comment, said Joe Klein, a network expert with the North American IPv6 Task Force and a senior security consultant with Honeywell. Klein believes that

the communications would not be detected by existing IPv4 devices, and that bot nets, among other threats, could use the technology for stealthier command and control channels.

Source: <http://www.securityfocus.com/news/11406?ref=rss>

39. *August 11, IDG News Service* — **Researchers: OpenOffice.org security insufficient.** With Microsoft Corp.'s Office suite now being targeted by hackers, researchers at the French Ministry of Defense say users of the OpenOffice.org software may be at even greater risk from computer viruses. "The general security of OpenOffice is insufficient," the researchers wrote in a paper entitled, "In-depth analysis of the viral threats with OpenOffice.org documents." The paper describes four proof-of-concept viruses that illustrate how maliciously encoded macros and templates could be created to compromise systems running the open-source software. "The viral hazard attached to OpenOffice.org is at least as high as that for the Microsoft Office suite, and even higher when considering some...aspects," they wrote. The report was written by researchers at the French Ministry of Defense's Signal Corps and was published in the Journal in Computer Virology, a Paris-based academic journal for computer scientists. Full-text report: <http://www.springerlink.com/content/2834v27846247480/fulltext.pdf> Source: [http://www.infoworld.com/article/06/08/11/HNopenofficesecurity\\_1.html](http://www.infoworld.com/article/06/08/11/HNopenofficesecurity_1.html)

### Internet Alert Dashboard

Current Port Attacks	
<b>Top 10 Target Ports</b>	1026 (win-rpc), 4672 (eMule), 445 (microsoft-ds), 32790 (---), 80 (www), 113 (auth), 135 (epmap), 5900 (vnc), 6346 (gnutella-svc), 139 (netbios-ssn) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
To report cyber infrastructure incidents or to request information, please contact US-CERT at <a href="mailto:soc@us-cert.gov">soc@us-cert.gov</a> or visit their Website: <a href="http://www.us-cert.gov">www.us-cert.gov</a> .	
Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <a href="https://www.it-isac.org/">https://www.it-isac.org/</a> .	

[\[Return to top\]](#)

## Commercial Facilities/Real Estate, Monument & Icons Sector

40. *August 11, Statesman Journal (OR)* — **Four pipe bombs found, destroyed in Oregon.** Three pipe bombs were discovered in separate public locations around Salem, OR, on Thursday, August 10, prompting police to issue a community-wide safety warning. A fourth pipe bomb was found Thursday evening in a parking lot of an electronics plant in Dallas, 15 miles west of downtown Salem. Dallas police Chief Jim Harper said officers were called about 7:45 p.m. PDT after a worker found the bomb outside the Tyco Electronics Dallas. The incident forced the evacuation of 60 to 70 workers. A state police bomb squad later rendered the bomb safe, Harper said. Of the bombs found in Salem, "all three are described as pipe bombs with some sort of wires," read a public notice issued by Salem police Thursday night. "The public should be cautioned not to touch any suspicious device, keep others away and immediately call the police." The FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives have been called in on the case, working in cooperation with Salem police and the Marion County Sheriff's Office, according to the notice.



Source: <http://www.statesmanjournal.com/apps/pbcs.dll/article?AID=/20060811/NEWS/608110315>

[\[Return to top\]](#)

## **General Sector**

Nothing to report.

[\[Return to top\]](#)

### **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.